WHAT WE CLAIM:

Sub a27

1. A cryptographic communication system comprising:

a plurality of user communication interfaces, each of said communication interface including:

a data receiver;

a string generator;

a data processor connected to said string generator; and

a memory connected to said string generator, said memory having stored a seed value;

a master station, said master station including:

a data transmitter

a second string generator;

a second data processor connected to said second string generator; and

a second memory connected to said second string generator, said second memory having stored said seed value,

2. The cryptographic communication system according to claim 1, wherein said string generator is a pseudo-random string generator, and wherein said second string generator is a pseudo-random string generator.

Sub A37

3. The cryptographic communication system according to claim 1,

wherein each of said plurality of user communication interface further includes a key block formation device, and

wherein said master station further includes a second key block formation device.

4. The cryptographic communication according to claim 1, wherein each of said plurality of user communication interface is connected to said master station through a communication network.

5. The cryptographic communication according to claim 1, wherein each of said plurality of user communication interface communicates with the master station via a wireless network.

6. The cryptographic communication system according to claim 1, wherein each seed value stored in a user communication interface is unique.

Sub A47

7. The cryptographic communication system according to claim 6,

wherein said second memory of said master station includes a plurality of seed values, and

wherein each of said seed values stored in said second memory correspond to a value stored by the memory of one of said plurality of said user communication interface.

8. The cryptographic communication system according to claim 1,

wherein said second memory of said master station stores a user address value for each of said plurality of user communication interface.

9. The cryptographic communication system according to claim 8, wherein each of the seed values stored in said second memory is referenced to by the user address value corresponding to the user communication interface in which the seed value is stored.

10. The cryptographic communication system according to claim 1,

wherein said second memory of said master station stores a user identification for each of said plurality of user communication interface.

11. The cryptographic communication system according to claim 10, wherein each of the seed values stored in said second memory is referenced to by the user identification corresponding to the user communication interface in which the seed value is stored.

12. The cryptographic communication system according to claim 1,

wherein each of said plurality of user communication interface further includes a data decryptor, and

wherein said master station further includes a master data encryptor.

13. The cryptographic communication system according to claim 1, wherein each of said plurality of user communication interface further includes a data encryptor, and

wherein said master station further includes a master data decryptor.

14. The cryptographic communication system according to claim 1, wherein the memory of at least one of said user communication interface includes a configurable common seed value, and

wherein the master memory of the master station includes said configurable common seed value.

15. The cryptographic communication system according to claim 1, wherein said master station can transmit data to each of said plurality of user communication interfaces.

16. A method of cryptographic communication comprising the steps of:

generating data strings;

forming a decryption key using at least one of said data strings;

receiving a signal; and

decrypting the received signal using said decryption key.

17. The method of cryptographic communication according to claim 16, wherein said data strings are generated in a pseudo-random order.

18. The method of cryptographic communication according to claim 16, further comprising the step of determining whether the received signal is encrypted.

19. The method of cryptographic communication according to claim 16, further comprising the step of selecting a seed value from which said data string is to be generated.

20. The method of cryptographic communication according to claim 16, further comprising the step of forming an encryption key using at least one of said generated data strings.

21. The method of cryptographic communication according to claim 20, further comprising the step of encrypting an output signal using said encryption key.

22. The method of cryptographic communication according to claim 20, further comprising the step of transmitting said output signal.

23. The method of cryptographic communication according to claim 16, wherein said data string is generated from a seed value.

24. The method of cryptographic communication according to claim 16, further comprising the step of transmitting a user address or a user identification.

25. A method of cryptographic communication comprising the steps of:

generating data strings;

forming an encryption key using at least one of said data strings;

encrypting a signal using said encryption keys; and

transmitting the signal.

26. The method of cryptographic communication according to claim 25, wherein said data strings are generated in a pseudo-random order.

27. The method of cryptographic communication according to claim 25, further comprising the step of determining whether to encrypt the signal prior to transmitting the signal signal.

28. The method of cryptographic communication according to claim 25, further comprising the step of receiving an incoming signal.

29. The method of cryptographic communication according to claim 25, further comprising the step of storing a user address.

30. The method of cryptographic communication according to claim 25, further comprising the step of storing a user identification.

31. The method of cryptographic communication according to claim 28, further comprising the step of determining whether said incoming signal is encrypted.

32. The method of cryptographic communication according to claim 29, further comprising the step of storing a seed value.

33. The method of cryptographic communication according to claim 32, further comprising the step of linking said user address to said seed value.

34. The method of cryptographic communication according to claim 32, further comprising the step of linking said user identification to said seed value.

35. The method of cryptographic communication according to claim 32, wherein said data strings are generated using said seed value.

36. The method of cryptographic communication according to claim 35, further comprising the step of forming a decryption key using at least one of said data strings.

37. The method of cryptographic communication according to claim 36, further comprising the step of decrypting said incoming signal using said decryption key.

38. A computer readable medium including executable instructions for causing a processor to perform a method of cryptographic communication, said method comprising the following steps:

generating data strings;

forming decryption keys using at least one of said data strings;

receiving a signal; and

decrypting the received signal using said decryption key.

39. The computer readable medium of claim 38, wherein said data strings are generated in a pseudo-random order.

40. The computer readable medium of claim 38, wherein said method further comprises the step of determining whether the received signal is encrypted.

41. The computer readable medium of claim 38, wherein said method further comprises the step of selecting a seed value from which said data string is to be generated.

42. The computer readable medium of claim 38, wherein said method further comprises the step of sending a user address.

43. The computer readable medium of claim 38, wherein said method further comprises the step of forming an encryption key using said generated data strings.

44. The computer readable medium of claim 43, wherein said method further comprises the step of encrypting an output signal using said encryption key.

45. The computer readable medium of claim 43, wherein said method further comprises the step of transmitting an output signal.

46. The computer readable medium of claim 41, wherein said data string is generated from the selected seed value.

47. The computer readable medium of claim 38, wherein said method further comprises the step of transmitting a user identification.

Sub K67 48. A computer readable medium including executable instructions for causing a processor to perform a method of cryptographic communication, said method comprising the following steps:

generating data strings;

forming an encryption key using said data strings;

encrypting programming signal using said encryption key; and

transmitting the programming signal.

49. The computer readable medium of claim 48, wherein said data strings are generated in a pseudo-random order.

50. The computer readable medium of claim 48, wherein said method further comprises the step of determining whether to encrypt the programming signal prior to transmitting said signal.

51. The computer readable medium of claim 48, wherein said method further comprises the step of receiving an incoming signal.

52. The computer readable medium of claim 48, wherein said method further comprises the step of storing a seed value.

53. The computer readable medium of claim 52, wherein said method further comprises the step of storing a user identification.

54. The computer readable medium of claim 51, wherein said method further comprises the step of determining whether said incoming signal is encrypted.

55. The computer readable medium of claim 52, wherein said method further comprises the step of storing a user address.

56. The computer readable medium of claim 55, wherein said method further comprises the step of linking said user address to said seed value.

57. The computer readable medium of claim 53, wherein said method further comprises the step of linking said user identification to said seed value.

58. The computer readable medium of claim 55, wherein said data strings are generated using said seed value.

59. The computer readable medium of claim 48, wherein said method further comprises the step of forming a decryption key using at least one of said data strings.

60. The computer readable medium of claim 59, wherein said method further comprises the step of decrypting said incoming signal using said decryption key.